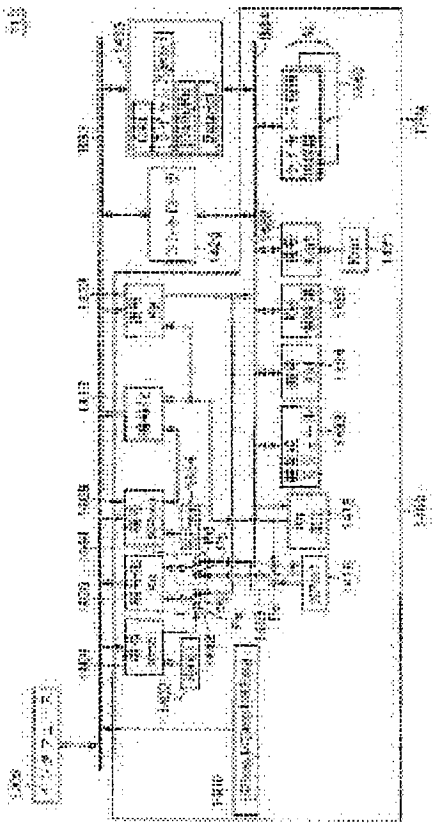
DATA RECORDING APPARATUS, AND DATA REPRODUCING DEVICE

Publication number: JP2002026890 (A)
Publication date: 2002-01-25
Inventor(s): HIOKI TOSHIAKI; KANAMORI YOSHIKAZU; HORI YOSHIHIRO
Applicant(s): SANYO ELECTRIC CO
Classification:
- international: ***G06F21/20; G06F15/00; H04L9/08; H04L9/32; H04N7/167; H04Q7/38;*** **G06F21/20; G06F15/00; H04L9/08; H04L9/32; H04N7/167; H04Q7/38;** (IPC1-7): H04L9/08; G06F15/00; H04L9/32; H04N7/167; H04Q7/38
- European:
Application number: JP20000202032 20000704
Priority number(s): JP20000202032 20000704

Abstract of **JP 2002026890 (A)**

PROBLEM TO BE SOLVED: To provide a data recording apparatus and a data reproducing device that can protect encrypted contents data by excluding external intrusions and to provide a terminal employing them. SOLUTION: A memory card 110 is provided with a key generating module 1432, an encryption section 1434 and a memory 1415. The key generating module 1432 generates a couple of a private encryption key and a public decoding key on the basis of information received from a portable telephone set onto which the memory card 110 is loaded. The memory 1415 stores the private encryption key and the open decoding key is transmitted to the data reproducing device and stored therein. In the case of reproducing encrypted contents data, the encryption section 1434 transmits a contents key encrypted by the private encryption key to the portable telephone set on the basis of the private encryption key read from the memory 1415 and the contents key.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－26890
（P2002－26890A）
(43)公開日　平成14年１月25日(2002.1.25)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　15/00	３３０Ｇ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６０１Ａ	５Ｃ０６４
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６０１Ｅ	５Ｋ０６７
Ｈ０４Ｎ　7/167			６７５Ｄ	

審査請求　未請求　請求項の数18　ＯＬ　（全 29 頁）　最終頁に続く

(21)出願番号　特願2000－202032(P2000－202032)

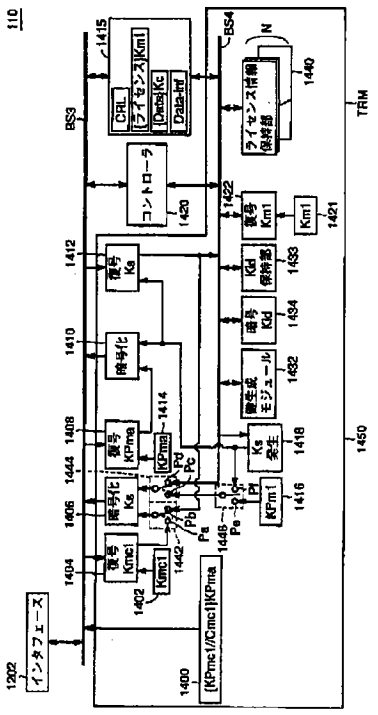
(22)出願日　平成12年７月４日(2000.7.4)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　日置　敏昭
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　金森　美和
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　データ記録装置、およびデータ再生装置

(57)【要約】
【課題】　暗号化されたコンテンツデータを外部からの進入を排除して保護できるデータ記録装置、データ再生装置、およびそれを用いた端末装置を提供する。
【解決手段】　メモリカード１１０は、鍵生成モジュール１４３２と、暗号部１４３４と、メモリ１４１５とを備える。鍵生成モジュール１４３２は、メモリカード１１０が装着された携帯電話機から入力された情報に基づいて一対の秘密暗号鍵と公開復号鍵とを生成する。秘密暗号鍵はメモリ１４１５に記録され、公開復号鍵はデータ再生装置へ送付されて保持される。暗号化コンテンツデータの再生時、暗号部１４３４は、メモリ１４１５から読出された秘密暗号鍵とコンテンツ鍵とに基づいて、秘密暗号鍵によって暗号化されたコンテンツ鍵を携帯電話機へ送信する。



1

【特許請求の範囲】

【請求項１】　バスと、

前記バスに接続され、外部とデータのやり取りを行なうインタフェース部と、

前記バスに接続された制御部と、

前記バスに接続され、ユーザからの指示に従って外部から入力される情報に基づいて暗号鍵と、前記暗号鍵によって暗号化されたデータを復号する復号鍵とを生成する鍵生成モジュールと、

前記バスに接続され、前記暗号鍵を保持する鍵保持部と、

前記バスに接続され、前記鍵保持部に保持された前記暗号鍵によって暗号化を行なう暗号部と、

前記バスに接続され、外部から入力されたデータを記録するメモリとを備え、

前記制御部は、前記鍵生成モジュールによって生成された前記暗号鍵を前記鍵保持部に記録し、前記復号鍵を前記インタフェース部を介して外部へ出力する、データ記録装置。

【請求項２】　ユーザからの出力要求により、

前記制御部は、前記メモリから前記データを取得して前記暗号部に与え、前記暗号部において前記鍵保持部に保持された暗号鍵によって暗号化されたデータを前記インタフェース部を介して外部へ出力する、請求項１に記載のデータ記録装置。

【請求項３】　前記データの入力時、

前記制御部は、前記暗号部において前記暗号鍵によって暗号化されたデータを前記メモリに記録する、請求項１に記載のデータ記録装置。

【請求項４】　ユーザからの出力要求により、

前記制御部は、前記メモリから前記暗号鍵によって暗号化された前記データを読出して前記インタフェース部を介して外部へ出力する、請求項３に記載のデータ記録装置。

【請求項５】　前記制御部は、前記データの出力先を認証する認証手段を有し、前記認証手段によって前記出力先が認証されたときに、前記データを出力する、請求項１から請求項４のいずれか１項に記載のデータ記録装置。

【請求項６】　データを暗号化した暗号化データと、前記暗号化データを復号して前記データを得るための復号鍵であるライセンスキーとを記録するデータ記録装置であって、

バスと、

前記バスに接続され、外部とやり取りを行なうインタフェース部と、

前記バスに接続された制御部と、

前記バスに接続され、ユーザからの指示に従って外部から入力される情報に基づいて暗号鍵と、前記暗号鍵によって暗号化されたデータを復号する復号鍵とを生成する

2

鍵生成モジュールと、

前記バスに接続され、前記暗号鍵を保持する鍵保持部と、

前記バスに接続され、前記鍵保持部に保持された前記暗号鍵によって暗号化を行なう暗号部と、

前記バスに接続され、外部から入力された前記ライセンスキーおよび暗号化データを記録するメモリとを備え、

前記制御部は、前記鍵生成モジュールによって生成された前記暗号鍵を前記鍵保持部に記録し、前記復号鍵を前記インタフェース部を介して外部へ出力する、データ記録装置。

【請求項７】　ユーザからの出力要求により、

前記制御部は、前記メモリから前記ライセンスキーを取得して前記暗号部に与え、前記暗号部において前記鍵保持部に保持された暗号鍵によって暗号化されたライセンスキーと前記メモリから取得した前記暗号化データとを前記インタフェース部を介して外部へ出力する、請求項６に記載のデータ記録装置。

【請求項８】　前記インタフェース部を介してライセンスキーが入力されたとき、

前記制御部は、前記暗号部において前記暗号鍵によって暗号化されたライセンスキーを前記メモリに記録する、請求項６に記載のデータ記録装置。

【請求項９】　ユーザからの出力要求により、

前記制御部は、前記メモリから前記暗号化データと、前記暗号鍵によって暗号化されたライセンスキーとを読出して前記インタフェース部を介して外部へ出力する、請求項８に記載のデータ記録装置。

【請求項１０】　前記制御部は、前記ライセンスキーの出力先を認証する認証手段を有し、前記認証手段により前記出力先が認証されたときに、前記ライセンスキーを出力する、請求項６から請求項９のいずれか１項に記載のデータ記録装置。

【請求項１１】　前記暗号鍵は、前記復号鍵と非対称である、請求項１または請求項６に記載のデータ記録装置。

【請求項１２】　データを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、前記暗号鍵によって暗号化された前記データと、前記復号鍵とを外部へ出力するデータ記録装置から前記データを再生するデータ再生装置であって、

バスと、

前記バスに接続され、ユーザが情報を入力する入力部と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのやり取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力され

た前記暗号鍵によって暗号化されたデータを、前記鍵メモリからの前記復号鍵によって復号する復号部とを含み、

前記制御部は、ユーザによって前記入力部から入力された情報を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記情報に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項１３】　データを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、前記暗号鍵によって暗号化された前記データと、前記復号鍵とを外部へ出力するデータ記録装置から前記データを再生するデータ再生装置であって、

バスと、

前記バスに接続され、ユーザが指示を入力する入力部と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのやり取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力された前記暗号鍵によって暗号化されたデータを、前記鍵メモリからの前記復号鍵によって復号する復号部とを含み、

前記制御部は、機器ＩＤを保持し、前記入力部からのユーザの指示によって前記機器ＩＤを前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記機器ＩＤに基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項１４】　前記制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータを前記メモリに記録するとともに、電話番号を保持し、前記入力部からのユーザの指示によって前記電話番号を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、請求項１３に記載のデータ再生装置。

【請求項１５】　データを暗号化した暗号化データと、前記暗号化データを復号して前記データを得るための復号鍵であるライセンスキーとを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、前記暗号鍵によって暗号化された前記ライセンスキーと、前記復号鍵とを外部へ出力するデータ記録装置から前記データを再生するデータ再生装置であって、

バスと、

前記バスに接続され、ユーザが情報を入力する入力部と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのやり取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力された前記暗号鍵によって暗号化されたライセンスキーを、前記鍵メモリからの前記復号鍵によって復号する第１の復号部と、

前記バスに接続され、前記データ記録装置から入力された前記暗号化データを、前記第１の復号部において復号されたライセンスキーによって復号する第２の復号部と、

前記第２の復号部において復号されたデータを再生する再生部とを含み、

前記制御部は、ユーザによって前記入力部から入力された情報を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記情報に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項１６】　データを暗号化した暗号化データと、前記暗号化データを復号して前記データを得るための復号鍵であるライセンスキーとを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、前記暗号鍵によって暗号化された前記ライセンスキーと、前記復号鍵とを外部へ出力するデータ記録装置から前記データを再生するデータ再生装置であって、

バスと、

前記バスに接続され、ユーザが指示を入力する入力部と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのやり取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力された前記暗号鍵によって暗号化されたライセンスキーを、前記鍵メモリからの前記復号鍵によって復号する第１の復号部と、

前記バスに接続され、前記データ記録装置から入力された前記暗号化データを、前記第１の復号部において復号されたライセンスキーによって復号する第２の復号部と、

前記第２の復号部において復号されたデータを再生する再生部とを含み、

前記制御部は、機器ＩＤを保持し、前記入力部からのユーザの指示によって前記機器ＩＤを前記インタフェース

部を介して前記データ記録装置へ出力し、前記データ記録装置が前記機器ＩＤに基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項１７】　前記制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータを前記メモリに記録するとともに、電話番号を保持し、前記入力部からのユーザの指示によって前記電話番号を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、請求項１６に記載のデータ再生装置。

【請求項１８】　前記暗号鍵は、前記復号鍵と非対称である、請求項１２から請求項１７のいずれか１項に記載のデータ再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムによって配信されたコンテンツデータを外部からの進入を排除して保護できるデータ記録装置およびデータ再生装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスキーを送信する。そして、暗号化コンテンツデータやライセンスキーを配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々に固有の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータとをメモリカードに送信する。そして、メモリカードは、受信したライセンスキーと暗号化コンテンツデータをメモリカードに記録する。

【００１２】メモリカードは、公開暗号鍵と非対称な秘密復号鍵を保持しており、この秘密復号鍵は、公開暗号鍵で暗号化されたデータを復号できる鍵である。メモリカードは、その秘密復号鍵を携帯電話機へ送信し、携帯電話機は暗号化されたライセンスキーを、受信した秘密復号鍵で復号し、暗号化コンテンツデータを復号したラ

イセンスキーによって復号してコンテンツデータを再生する。

【００１３】上記のようなデータ配信システムにおいては、配信サーバは、ライセンスキーの配信に対して課金し、暗号化した状態でライセンスキーや暗号化コンテンツデータをメモリカードへ送信するので、著作権は十分に保護されている。また、暗号化コンテンツデータを受信した携帯電話機のユーザがその暗号化コンテンツデータを他人にコピーしても、その他人は暗号化コンテンツデータを復号するライセンスキーを取得できないので、そのままでは暗号化コンテンツデータを再生できない。他人が暗号化コンテンツデータを再生するには、配信サーバへアクセスし、別途、料金を支払ってライセンスキーを購入する必要がある。したがって、受信した暗号化コンテンツデータを他人がコピーすることは自由であるが、その他人は、新たにライセンスキーを購入しなければならないので、自由なコピーを許容しながら著作権をも保護している。

【００１４】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータを再生するためにメモリカードと携帯電話機との間でデータのやり取りを行なう場合、メモリカードで発生させた共通鍵と携帯電話機で発生させた共通鍵とによって暗号化を行なっている。したがって、メモリカードおよび携帯電話機に固有の鍵を用いてデータのやり取りを行なうことができず、外部からの進入に対して十分な保護がなされていなかった。

【００１５】そこで、本発明はかかる問題を解決するためになされたものであり、その目的は、暗号化されたコンテンツデータを外部からの進入を排除して保護できるデータ記録装置、およびデータ再生装置を提供することである。

【００１６】

【課題を解決するための手段および発明の効果】この発明によるデータ記録装置は、バスと、バスに接続され、外部とデータのやり取りを行なうインタフェース部と、バスに接続された制御部と、バスに接続され、ユーザからの指示に従って外部から入力される情報に基づいて暗号鍵と、暗号鍵によって暗号化されたデータを復号する復号鍵とを生成する鍵生成モジュールと、バスに接続され、暗号鍵を保持する鍵保持部と、バスに接続され、鍵保持部に保持された暗号鍵によって暗号化を行なう暗号部と、バスに接続され、外部から入力されたデータを記録するメモリとを備え、制御部は、鍵生成モジュールによって生成された暗号鍵を鍵保持部に記録し、復号鍵を前インタフェース部を介して外部へ出力する。

【００１７】この発明によるデータ記録装置においては、データ記録装置の一例であるメモリカードが装着された携帯電話機からユーザによって情報が入力される。そうすると、メモリカードの制御部は携帯電話機から情報を入力して鍵生成モジュールに入力する。そうすると、鍵生成モジュールは、入力された情報に基づいて暗号鍵と復号鍵とを生成する。そして、生成された暗号鍵は鍵保持部に保持され、復号鍵はインタフェース部を介して外部へ出力される。

【００１８】したがって、この発明によれば、データ記録装置は、装着された端末装置から入力された情報に基づいて暗号鍵と復号鍵とを生成できる。その結果、外部からの進入を防止してデータ記録装置と端末装置とのデータのやり取りを行なうことができる。

【００１９】好ましくは、ユーザからの出力要求により、制御部は、メモリからデータを取得して暗号部に与え、暗号部において鍵保持部に保持された暗号鍵によって暗号化されたデータをインタフェース部を介して外部へ出力する。

【００２０】データ記録装置が装着された端末装置を介してユーザから出力要求があったとき、制御部はメモリからデータを取得して暗号部へ入力する。そして、暗号部は暗号鍵によってデータを暗号化する。制御部は暗号鍵によって暗号化されたデータを外部へ出力する。そうすると、データ再生装置は、暗号鍵によって暗号化されたデータを復号鍵によって復号して再生する。

【００２１】したがって、この発明によれば、データ記録装置が装着された端末装置から入力された情報に基づいて生成された暗号鍵と復号鍵とを用いてデータを端末装置へ送信して再生できる。その結果、データの再生過程に外部から進入できず、データを十分に保護できる。

【００２２】好ましくは、データの入力時、制御部は、暗号部において暗号鍵によって暗号化されたデータをメモリに記録する。

【００２３】データが入力されるとき、暗号部は、鍵保持部から読出された暗号鍵によってデータを暗号化する。そして、制御部は、暗号鍵によって暗号化されたデータをメモリに記録する。

【００２４】したがって、この発明によれば、データ記録装置に記録されたデータを再生するとき、データに外部から容易にアクセスできず、データを十分に保護できる。

【００２５】好ましくは、ユーザからの出力要求により、制御部は、メモリから暗号鍵によって暗号化されたデータを読出してインタフェース部を介して外部へ出力する。

【００２６】ユーザから出力要求があると、制御部はメモリに記録された暗号化データを読出してデータ再生装置へ出力する。そして、データ再生装置において、暗号化データは復号鍵によって復号されて再生される。

【００２７】したがって、この発明によれば、暗号化データの再生時、暗号化データをメモリから読出してデータ再生装置へ送信すれば良く、迅速な再生動作を実現できる。

【００２８】好ましくは、データ記録装置の制御部は、データの出力先を認証する認証手段を有し、認証手段によって出力先が認証されたときに、データを出力する。

【００２９】データ記録装置に記録されたデータを再生するとき、データの出力先が正規の出力先であることが確認されてから、その出力先へデータが出力される。

【００３０】したがって、この発明によれば、正規な出力先へのみデータを出力でき、データ記録装置に記録されたデータに対する十分な保護が可能である。

【００３１】また、この発明によるデータ記録装置は、データを暗号化した暗号化データと、暗号化データを復号してデータを得るための復号鍵であるライセンスキーとを記録するデータ記録装置であって、バスと、バスに接続され、外部とやり取りを行なうインタフェース部と、バスに接続された制御部と、バスに接続され、ユーザからの指示に従って外部から入力される情報に基づいて暗号鍵と、暗号鍵によって暗号化されたデータを復号する復号鍵とを生成する鍵生成モジュールと、バスに接続され、暗号鍵を保持する鍵保持部と、バスに接続され、鍵保持部に保持された暗号鍵によって暗号化を行なう暗号部と、バスに接続され、外部から入力されたライセンスキーおよび暗号化データを記録するメモリとを備え、制御部は、鍵生成モジュールによって生成された暗号鍵を鍵保持部に記録し、復号鍵をインタフェース部を介して外部へ出力する。

【００３２】この発明によるデータ記録装置においては、データ記録装置の一例であるメモリカードが装着された携帯電話機からユーザの指示によって情報が入力される。そうすると、メモリカードの制御部は携帯電話機から情報を入力して鍵生成モジュールに入力する。そうすると、鍵生成モジュールは、入力された情報に基づいて暗号鍵と復号鍵とを生成する。そして、生成された暗号鍵は鍵保持部に保持され、復号鍵はインタフェース部を介して外部へ出力される。また、メモリには暗号化データと、その暗号化データを復号するためのライセンスキーとが記録される。

【００３３】したがって、この発明によれば、データ記録装置は、装着された端末装置から入力された情報に基づいて暗号鍵と復号鍵とを生成できる。その結果、外部からの進入を防止してデータ記録装置と端末装置との暗号化データのやり取りを行なうことができる。

【００３４】好ましくは、ユーザからの出力要求により、制御部は、メモリからライセンスキーを取得して暗号部に与え、暗号部において鍵保持部に保持された暗号鍵によって暗号化されたライセンスキーとメモリから取得した暗号化データとをインタフェース部を介して外部へ出力する。

【００３５】データ記録装置が装着された端末装置を介してユーザから出力要求があったとき、制御部はメモリからライセンスキーを取得して暗号部へ入力する。そして、暗号部は暗号鍵によってライセンスキーを暗号化する。制御部は暗号鍵によって暗号化されたライセンスキーを外部へ出力する。そうすると、データ再生装置は、暗号鍵によって暗号化されたライセンスキーを復号鍵によって復号し、その復号されたライセンスキーを用いて暗号化データを復号して再生する。

【００３６】したがって、この発明によれば、データ記録装置が装着された端末装置から入力された情報に基づいて生成された暗号鍵と復号鍵とを用いてライセンスキーを暗号化し、その暗号化されたライセンスキーを端末装置へ送信して再生できる。その結果、暗号化データの再生過程に外部から進入できず、データを十分に保護できる。

【００３７】好ましくは、インタフェース部を介してライセンスキーが入力されたとき、制御部は、暗号部において暗号鍵によって暗号化されたライセンスキーをメモリに記録する。

【００３８】ライセンスキーが入力されるとき、暗号部は、鍵保持部から読出された暗号鍵によってデータを暗号化する。そして、制御部は、暗号鍵によって暗号化されたライセンスキーをメモリに記録する。

【００３９】したがって、この発明によれば、外部から入力されたライセンスキーに対してデータ記録装置において生成された暗号鍵を用いて暗号化を行なうことができる。その結果、暗号化データの再生過程で用いるライセンスキーを、外部からの進入を防止してデータ再生装置へ送信することができ、暗号化データの十分な保護が可能である。

【００４０】好ましくは、ユーザからの出力要求により、制御部は、メモリから暗号化データと、暗号鍵によって暗号化されたライセンスキーとを読出してインタフェース部を介して外部へ出力する。

【００４１】ユーザから出力要求があると、制御部はメモリに記録された暗号化データと、データ記録装置において生成された暗号鍵によって暗号化されたライセンスキーとを読出して外部へ出力する。そして、たとえば、データ再生装置において、暗号化されたライセンスキーは復号鍵によって復号され、その復号されたライセンスキーによって暗号化データが復号されてデータが再生される。

【００４２】したがって、この発明によれば、暗号化データの再生時、暗号化されたライセンスキーと、暗号化データとをメモリから読出してデータ再生装置へ送信すれば良く、迅速な再生動作を実現できる。

【００４３】好ましくは、データ記録装置の制御部は、ライセンスキーの出力先を認証する認証手段を有し、認証手段により出力先が認証されたときに、ライセンスキーを出力する。

【００４４】データ記録装置に記録された暗号化データを再生するとき、暗号化データの出力先が正規の出力先

であることが確認されてから、その出力先へ暗号化データが出力される。

【００４５】したがって、この発明によれば、正規な出力先へのみ暗号化データを出力でき、データ記録装置に記録された暗号化データに対する十分な保護が可能である。

【００４６】好ましくは、暗号鍵は、復号鍵と非対称である。データ記録装置は、入力された情報に基づいて非対称な暗号鍵と復号鍵とを生成する。

【００４７】したがって、暗号鍵を秘密鍵として、また復号鍵を公開鍵として取り扱うことができる。その結果、復号鍵だけを再生装置へ送信して保持し、再生時に暗号鍵によって暗号化されたデータを再生装置へ送信すればよく、データを十分に保護できる。

【００４８】また、この発明によるデータ再生装置は、データを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたデータと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが情報を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたデータを、鍵メモリからの復号鍵によって復号する復号部とを含み、制御部は、ユーザによって入力部から入力された情報をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が情報に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【００４９】この発明によるデータ再生装置においては、ユーザによって情報が入力されると、その入力された情報はデータ記録装置へ送信され、データ記録装置において情報に基づいて一対の暗号鍵と復号鍵とが生成される。そして、データ再生装置は、生成された復号鍵をデータ記録装置から受取り、鍵メモリに保持する。

【００５０】したがって、この発明によれば、データ再生装置は、入力した情報に基づいて生成された復号鍵を保持できる。その結果、データの再生時、データ記録装置から暗号鍵によって暗号化されたデータのみを受け取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【００５１】また、この発明によるデータ再生装置は、データを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたデータと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが指示を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたデータを、鍵メモリからの復号鍵によって復号する復号部とを含み、制御部は、機器ＩＤを保持し、入力部からのユーザの指示によって機器ＩＤをインタフェース部を介してデータ記録装置へ出力し、データ記録装置が機器ＩＤに基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【００５２】この発明によるデータ再生装置においては、そのデータ再生装置の機器ＩＤがデータ記録装置へ送信され、データ記録装置において機器ＩＤに基づいて一対の暗号鍵と復号鍵とが生成される。そして、データ再生装置は、生成された復号鍵をデータ記録装置から受取り、鍵メモリに保持する。

【００５３】したがって、この発明によれば、データ再生装置に固有の情報に基づいて一対の暗号鍵と復号鍵とを生成できる。

【００５４】また、データ再生装置は、データの再生時、データ記録装置から暗号鍵によって暗号化されたデータのみを受け取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【００５５】好ましくは、データ再生装置の制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータをメモリに記録するとともに、電話番号を保持し、入力部からのユーザの指示によって電話番号をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵を前記インタフェース部を介して取得して鍵メモリに入力する。

【００５６】データ再生装置の制御部は、ユーザからの指示によって保持している電話番号をデータ記録装置へ送信する。そうすると、データ記録装置は、送信された電話番号に基づいて一対の暗号鍵と復号鍵とを生成する。そして、データ再生装置は、生成された復号鍵をデータ記録装置から受取り、鍵メモリに保持する。

【００５７】したがって、この発明によれば、データ再生装置に固有の情報に基づいて一対の暗号鍵と復号鍵とを生成できる。

【００５８】また、この発明によれば、データ再生装置は、データの再生時、データ記録装置から暗号鍵によって暗号化されたデータのみを受け取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【００５９】また、この発明によるデータ再生装置は、データを暗号化した暗号化データと、暗号化データを復号してデータを得るための復号鍵であるライセンスキー

13

とを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたライセンスキーと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが情報を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたライセンスキーを、鍵メモリからの復号鍵によって復号する第１の復号部と、バスに接続され、データ記録装置から入力された暗号化データを、第１の復号部において復号されたライセンスキーによって復号する第２の復号部と、第２の復号部において復号されたデータを再生する再生部とを含み、制御部は、ユーザによって入力部から入力された情報をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が情報に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【００６０】この発明によるデータ再生装置は、入力された情報をデータ記録装置へ送信し、データ記録装置においてその送信した情報に基づいて生成された復号鍵をデータ記録装置から受取って鍵メモリに保持する。そして、暗号化データの再生時、データ再生装置は、暗号鍵によって暗号化されたライセンスキーと、暗号化データとをデータ記録装置から受取り、暗号化されたライセンスキーを復号鍵によって復号し、その復号したライセンスキーによって暗号化データを復号してデータを再生する。

【００６１】したがって、この発明によれば、データ再生装置は、データの再生時、暗号化データと、暗号鍵によって暗号化されたライセンスキーとをデータ記録装置から受取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【００６２】この発明によるデータ再生装置は、データを暗号化した暗号化データと、暗号化データを復号してデータを得るための復号鍵であるライセンスキーとを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたライセンスキーと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが指示を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたライセンスキーを、鍵メモリからの復号鍵によって復号する第１の

14

復号部と、バスに接続され、データ記録装置から入力された暗号化データを、第１の復号部において復号されたライセンスキーによって復号する第２の復号部と、第２の復号部において復号されたデータを再生する再生部とを含み、制御部は、機器ＩＤを保持し、入力部からのユーザの指示によって機器ＩＤをインタフェース部を介してデータ記録装置へ出力し、データ記録装置が機器ＩＤに基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【００６３】この発明によるデータ再生装置は、保持する機器ＩＤをデータ記録装置へ送信し、データ記録装置においてその送信した機器ＩＤに基づいて生成された復号鍵をデータ記録装置から受取って鍵メモリに保持する。そして、暗号化データの再生時、データ再生装置は、暗号鍵によって暗号化されたライセンスキーと、暗号化データとをデータ記録装置から受取り、暗号化されたライセンスキーを復号鍵によって復号し、その復号したライセンスキーによって暗号化データを復号してデータを再生する。

【００６４】したがって、この発明によれば、データ再生装置に固有の機器ＩＤに基づいて暗号鍵と復号鍵とを生成できる。

【００６５】また、この発明によれば、データ再生装置は、データの再生時、暗号化データと、暗号鍵によって暗号化されたライセンスキーとをデータ記録装置から受取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【００６６】好ましくは、データ再生装置の制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータをメモリに記録するとともに、電話番号を保持し、入力部からのユーザの指示によって電話番号をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【００６７】この発明によるデータ再生装置は、保持する電話番号をデータ記録装置へ送信し、データ記録装置においてその送信した電話番号に基づいて生成された復号鍵をデータ記録装置から受取って鍵メモリに保持する。そして、暗号化データの再生時、データ再生装置は、暗号鍵によって暗号化されたライセンスキーと、暗号化データとをデータ記録装置から受取り、暗号化されたライセンスキーを復号鍵によって復号し、その復号したライセンスキーによって暗号化データを復号してデータを再生する。

【００６８】したがって、この発明によれば、データ再生装置に固有の電話番号に基づいて暗号鍵と復号鍵とを生成できる。

【００６９】また、この発明によれば、データ再生装置

は、データの再生時、暗号化データと、暗号鍵によって暗号化されたライセンスキーとをデータ記録装置から受取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【００７０】好ましくは、暗号鍵は、復号鍵と非対称である。データ記録装置は、入力された情報に基づいて非対称な暗号鍵と復号鍵とを生成する。

【００７１】したがって、暗号鍵を秘密鍵として、また復号鍵を公開鍵として取り扱うことができる。その結果、復号鍵だけを再生装置へ送信して保持し、再生時に暗号鍵によって暗号化されたデータを再生装置へ送信すればよく、データを十分に保護できる。

【００７２】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００７３】図１は、本発明によるデータ再生装置が再生の対象とする暗号化コンテンツデータをデータ記録装置（メモリカード）へ配信するデータ配信システムの全体構成を概略的に説明するための概念図である。

【００７４】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても、さらには、他の情報通信網を介して配信する場合においても適用することが可能なものである。

【００７５】図１を参照して、著作権の存在する音楽データを管理するライセンスサーバ１０は、データ配信を求めてアクセスしてきた携帯電話ユーザの携帯電話機に装着されたメモリカードが正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータを与える。

【００７６】配信キャリア２０は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ１０に中継する。ライセンスサーバ１０は、配信リクエストがあると、認証サーバ１２によりメモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア２０の携帯電話網を介して、各携帯電話ユーザの携帯電話機を介して接続されたメモリカードに対してコンテンツデータを配信する。

【００７７】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取って、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００７８】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００７９】以下では、このようなライセンスサーバ１０と配信キャリア２０と併せて、配信サーバ３０と総称することにする。

【００８０】また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００８１】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００８２】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００８３】しかも、このようなコンテンツデータの配信は、携帯電話機網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【００８４】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話ユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号化鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００８５】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００８６】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００８７】まず、配信サーバ３０より配信されるデータについて説明する。Ｄａｔａは、音楽データ等のコンテンツデータである。コンテンツデータＤａｔａには、ライセンスキーＫｃで復号可能な暗号化が施される。ライセンスキーＫｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

【００８８】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００８９】さらに、配信サーバ３０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、ライセンス情報としては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１および再生回路における制御情報である再生回路制御情報ＡＣ２等が存在する。以後、ライセンスキーＫｃとコンテンツＩＤとライセンスＩＤとアクセス制御情報ＡＣ１と再生回路制御情報ＡＣ２とを併せて、ライセンスと総称することとする。

【００９０】図３は、図１に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【００９１】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツ再生回路（携帯電話機）のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００９２】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止されるコンテンツ再生回路およびメモリカードのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。

【００９３】禁止クラスリストデータＣＲＬは、配信サーバ３０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データＣＲＬ＿ｄａｔの配信サーバ３０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬが書替えられる構成とする。また、禁止クラスリストのバージョンについては、ＣＲＬ＿ｖｅｒをメモリカード側より出力し、これを配信サーバ３０側で確認することによってバージョン管理を実行する。差分データＣＲＬ＿ｄａｔには新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【００９４】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカード内でおいても保持運用することによって、クラス固有すなわちコンテンツ再生回路およびメモリカードの種類に固有の復号鍵の破られた、コンテンツ再生回路およびメモリカードへのライセンスキーの供給を禁止する。このため、コンテンツ再生回路ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【００９５】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリ回路内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【００９６】コンテンツ再生回路（携帯電話機）およびメモリカードには固有の公開暗号鍵ＫＰｐｎおよびＫＰｍｃｍがそれぞれ設けられ、公開暗号鍵ＫＰｐｎおよびＫＰｍｃｍはコンテンツ再生回路（携帯電話機）の固有の秘密復号鍵Ｋｐｎおよびメモリカード固有の秘密復号鍵Ｋｍｃｍによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【００９７】また、再生回路およびメモリカードのクラス証明書として、ＣｒｔｆｎおよびＣｍｃｍがそれぞれ設けられる。これらのクラス証明書は、メモリカードおよびコンテンツ再生部（携帯電話機）のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が拾得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【００９８】これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｃｍ／／Ｃｍｃｍ｝ＫＰｍａの形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。後ほど詳細に説明するが、ＫＰｍａは配信システム全体で共通の公開認証鍵である。

【００９９】図４は、図１に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

19

【０１００】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ３０、携帯電話機１００、メモリカード１１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【０１０１】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【０１０２】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションごとに発生し、セッションキーＫｓ３は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【０１０３】また、メモリカード１００内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍと、公開暗号鍵ＫＰｍで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍが存在する。

【０１０４】さらに、携帯電話機のＩＤ、携帯電話機の電話番号、時刻等の携帯電話機から選られる情報に基づいて生成され、暗号化コンテンツデータの再生時にメモリカードと携帯電話機とのデータのやり取りに用いられる一対の公開暗号鍵ＫＰｉｄと秘密復号鍵Ｋｉｄが存在する。

【０１０５】図５は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。

【０１０６】ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４、課金データベース３０２およびＣＲＬデータベース３０６からのデータをデータバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

20

【０１０７】データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための復号することでその正当性が認証できる状態に暗号化した認証データ｛ＫＰｍｃｍ／／Ｃｍｃｍ｝ＫＰｍａを通信装置３５０およびデータバスＢＳ１を介して受けて、公開認証鍵ＫＰｍａによる復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｍを用いて暗号化して、データバスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをデータバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【０１０８】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンスキーＫｃおよび再生回路制御情報ＡＣ２を、復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してデータバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【０１０９】ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１１０】図６は、図１に示した携帯電話機１００の構成、すなわち、本発明の実施の形態によるデータ再生装置を含む携帯電話機の構成を説明するための概略ブロック図である。

【０１１１】携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。なお、コントローラ１１０６は、機器ＩＤ、電話番号等の携帯電話機１００から得られる情報を保持する。

【０１１２】携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるための操作ボタン部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データベースＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部とのデ

ータのやり取りを行なう外部インタフェース部１１０７とを含む。

【０１１３】携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリカードインタフェースと、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｒｔｆ１を公開認証鍵ＫＰｍａで復号することでその正当性が認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを保持する認証データ保持部１５００を含む。

【０１１４】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるＫｐ１、およびＫｐ２を保持するＫｐｘ保持部１５０２と、データバスＢＳ２から受けたデータをＫｐ１またはＫｐ２によって復号しメモリカードによって発生されたセッションキーＫｓ２を得る復号処理部１５０４と、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でデータバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、生成されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化しデータバスＢＳ２に出力する暗号処理部１５０６と、データバスＢＳ２上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１５１０とを含む。

【０１１５】携帯電話機１００は、さらに、メモリカード１１０にて発生した対をなす秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄのうちの１つである公開復号鍵ＫＰｉｄをメモリカード１１０から受けて保持する鍵メモリ１５１２と、復号処理部１５１０の出力である秘密暗号鍵Ｋｉｄにて暗号化されたライセンスキーおよび再生回路制御情報｛Ｋｃ／／ＡＣ２｝ＫＰｉｄを鍵メモリ１５１２に保持された公開復号鍵ＫＰｉｄによって復号処理を行ない、復号したライセンスキーＫｃを復号処理部１５１６へ、再生回路制御情報ＡＣ２をデータバスＢＳ２を介してコントローラ１１０６へ出力する復号処理部１５１４を含む。

【０１１６】携帯電話機１００は、さらに、データバスＢＳ２より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１５１０より取得したライセンスキーＫｃによって復号しコンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、音声再生部１１１２の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１１１３と、ＤＡ変換器１１１３とＤＡ変換器１５１９との出力を受けて、動作モードに応じて選択的に端子１１１４または端子１５２０から出力するためのスイッチ１５２１と、スイッチ１５２１の出力を受けて、データを増幅する増幅器１５２２と、増幅器１５２２の出力を受けてヘッドホン１３０と接続するための接続端子１５３０とを含む。

【０１１７】なお、図６においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１１８】また、携帯電話ユーザの利便性を図るために、携帯電話機１００のうち、通話処理に関するブロックを除いた、図６において実線で囲まれる、コンテンツデータの配信および再生に関するブロック全体を音楽再生モジュール１５５０として、着脱可能なモジュール化する構成を採用することも可能である。

【０１１９】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１２０】図７は、図６に示したメモリカード１１０の構成を説明するための概略ブロック図である。

【０１２１】既に説明したように、メモリカードの固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃｍおよびＫｍｃｍが設けられ、メモリカードのクラス証明書Ｃｍｃｍが設けられるが、メモリカード１１０においては、これらは自然数ｍ＝１でそれぞれ表わされるものとする。

【０１２２】したがって、メモリカード１１０は、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ１を保持するＫｍｃ保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Ｋｍ１を保持するＫｍ１保持部１４２１と、Ｋｍ１によって復号可能な公開暗号鍵ＫＰｍ１を保持するＫＰｍ１保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される公開暗号鍵ＫＰｍｃ1およびクラス証明書Ｃｍｃ１を公開認証鍵ＫＰｍａで復号することでその正当性が認証できる状態に暗号化した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａとして保持する。

【０１２３】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

【０１２４】メモリカード１１０は、さらに、メモリカードインタフェースとの間で信号をインタフェース１２

０２を介して授受するデータバスＢＳ３と、データバスＢＳ３にメモリカードインタフェースから与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Ｋｍｃ１をＫｍｃ１保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ１を接点Ｐａに出力する復号処理部１４０４と、ＫＰｍａ保持部１４１４から公開認証鍵ＫＰｍａを受けて、データバスＢＳ３に与えられるデータを公開認証鍵ＫＰｍａによる復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してデータバスＢＳ３に出力する暗号化処理部１４０６とを含む。

【０１２５】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｎもしくはＫＰｍｃｍによって暗号化してデータバスＢＳ３に送出する暗号化処理部１４１０と、ＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号し、復号結果をデータバスＢＳ４に送出する復号処理部１４１２とを含む。

【０１２６】メモリカード１１０は、さらに、携帯電話機１００のコントローラ１１０６が保持する機器ＩＤ、電話番号等の情報をインタフェース１２０２およびデータバスＢＳ３を介して入力し、入力した情報に基づいて秘密暗号鍵Ｋｉｄと、秘密暗号鍵Ｋｉｄと対を成す公開復号鍵ＫＰｉｄとを生成する鍵生成モジュール１４３２と、秘密暗号鍵Ｋｉｄを保持するＫｉｄ保持部１４３３と、Ｋｉｄ保持部１４３３に保持された秘密暗号鍵Ｋｉｄによって暗号処理を行なう暗号処理部１４３４とを含む。

【０１２７】メモリカード１１０は、さらに、データバスＢＳ４上のデータを公開暗号鍵ＫＰｍ１と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号するための復号処理部１４２２と、公開暗号鍵ＫＰｍ１で暗号化されている、ライセンスキーＫｃ、再生回路制御情報ＡＣ２および再生情報（コンテンツＩＤ，ライセンスＩＤ，アクセス制御情報ＡＣ１）と、暗号化されていない禁止クラスリストのバージョン更新のための差分データＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬとをデータバスＢＳ４より受けて格納するとともに、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをデータバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。

【０１２８】メモリカード１１０は、さらに、復号処理部１４２２によって得られるメモリカード１１０にて参照されるライセンスの一部、すなわち、ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を保持するためのライセンス情報保持部１４４０と、データバスＢＳ３を介して外部との間でデータ授受を行ない、データバスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１２９】ライセンス情報保持部１４４０は、データバスＢＳ４との間でライセンスＩＤ、データコンテンツＩＤデータおよびアクセス制限情報ＡＣ１のデータの授受が可能である。ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

【０１３０】なお、図７において、実線で囲んだ領域は、ライセンス保護モジュール１４５０を構成する。また、メモリ１４１５は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）である。

【０１３１】次に、図１に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【０１３２】図８および図９は、図１に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１および第２のフローチャートである。

【０１３３】図８および図９においては、携帯電話ユーザが、メモリカード１１０を用いることで、携帯電話機１００を介して配信サーバ３０から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【０１３４】まず、携帯電話ユーザの携帯電話機１００から携帯電話ユーザにより操作ボタン部１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【０１３５】メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａが出力される（ステップＳ１０２）。

【０１３６】携帯電話機１００は、メモリカード１１０から受理した認証のための認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

【０１３７】配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａ、ライセンス購入条件データＡＣを受信し、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰｍａで復号処理を実行する（ステップＳ１０８）。

【０１３８】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍｃ１と証明書Ｃｍｃ１を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１０）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を承認し、受理する。そして次の処理（ステップＳ１１２）に移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を受理しないで処理を終了する（ステップＳ１７０）。

【０１３９】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであると承認されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍｃ１が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

【０１４０】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

【０１４１】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ１によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

【０１４２】暗号化されたセッションキーＫｓ１は、｛Ｋｓ１｝Ｋｍｃ１として、データバスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

【０１４３】携帯電話機１００が、暗号化されたセッションキー｛Ｋｓ１｝Ｋｍｃ１を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリカードインタフェースを介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ１により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１２０）。

【０１４４】コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカードにおいて配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

【０１４５】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストの状態（バージョン）に関連する情報として、リストのバージョンデータＣＲＬ＿ｖｅｒをメモリ１４１５から抽出してデータバスＢＳ４に出力する。

【０１４６】暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍ１および禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１をデータバスＢＳ３に出力する（ステップＳ１２２）。

【０１４７】データバスＢＳ３に出力された暗号データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１は、データバスＢＳ３からインタフェース１２０２およびメモリカードインタフェースを介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

【０１４８】配信サーバ３０は、暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍ１およびメモリカード１１０における禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを受理する（ステップＳ１２６）。

【０１４９】禁止クラスリストのバージョン情報ＣＲＬ＿ｖｅｒは、データバスＢＳ１を介して配信制御部３１５に送られ、配信制御部３１５は、受理したバージョンデータＣＲＬ＿ｖｅｒに従って、当該ＣＲＬ＿ｖｅｒのバージョンとＣＲＬデータベース３０６内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データＣＲＬ＿ｄａｔを生成する（ステップＳ１２８）。

【０１５０】さらに、配線制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件データＡＣに従って、ライセンスＩＤ、アクセス制限情報ＡＣ１および再生回路制御情報ＡＣ２を生成する（ステップＳ１３０）。さらに、暗号化コンテンツデータを復号するためのライセンスキーＫｃを情報データベース３０４より取得する（ステップＳ１３２）。

【０１５１】図９を参照して、配信制御部３１５は、生成したライセンス、すなわち、ライセンスキーＫｃを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ１によってライセンスキーＫｃ、再生回路制御情報ＡＣ２、ライセンスＩＤ、コンテンツＩＤ、およびアクセス制限情報ＡＣ１を暗号化する（ステップＳ１３６）。暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がデータバスＢＳ１を介して供給する禁止クラスリストの差分データＣＲＬ＿ｄａｔとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、データバスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

【０１５２】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１５３】携帯電話機１００は、送信された暗号化ライセンス｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ２を受信し（ステップＳ１４０）、メモリカード１１０においては、メモリカードインタフェースを介して、データバスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてデータバスＢＳ３の受信データを復号しデータバスＢＳ４に出力する（ステップＳ１４２）。

【０１５４】この段階で、データバスＢＳ４には、Ｋｍ１保持部１４２１に保持される秘密復号鍵Ｋｍ１で復号可能な暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１と、ＣＲＬ＿ｄａｔとが出力される。コントローラ１４２０の指示によって、暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１は、メモリ１４１５に記録される（ステップＳ１４４）。一方、暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１は、復号処理部１４２２において、秘密復号鍵Ｋｍ１によって復号され、ライセンスのうち、メモリカード１１０内で参照されるライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１のみが受理される（ステップＳ１４６）。

【０１５５】コントローラ１４２０は、受理したＣＲＬ＿ｄａｔに基づいて、メモリ１４１５内の禁止クラスリストデータＣＲＬおよびそのバージョンを更新する（ステップＳ１４８）。さらに、メモリ内で参照されるライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１については、ライセンス情報保持部１４４０に記録される（ステップＳ１５０）。

【０１５６】ステップＳ１５０までの処理がメモリ回路で正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ１５２）。

【０１５７】配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを取得して、これらのデータをデータバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１５４）。

【０１５８】携帯電話機１００は、｛Ｄａｔａ｝Ｋｃ／／Ｄａｔａ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを受理する（ステップＳ１５６）。暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆはメモリカードインタフェースおよびインタフェース１２０２を介してメモリカード１１０のデータバスＢＳ３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆがそのままメモリ１４１５に記録される（ステップＳ１５８）。

【０１５９】さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ１６０）、配信サーバ３０で配信受理を受信すると（ステップＳ１６２）、課金データベース３０２への課金データの格納等を伴って、配信終了の処理が実行され（ステップＳ１６４）、全体の処理が終了する（ステップＳ１７０）。

【０１６０】このようにして、携帯電話機１００のメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍｃ１とともに暗号化して送信できた公開暗号鍵Ｋｍｃ１が有効であることを確認した上で、それぞれのクラス証明書Ｃｍｃ１が禁止クラスリスト、すなわち、公開暗号鍵Ｋｍｃ１による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１６１】図１０を参照して、携帯電話機１００から得られる情報に基づいてメモリカード１１０において一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとを生成する動作について説明する。

【０１６２】鍵生成が開始されると、ユーザは携帯電話機１００の操作ボタン部１１０８から任意のデータを入力する。そうすると、コントローラ１１０６は、メモリ

カードインタフェースを介して入力されたデータをメモリカード１１０に送付するとともにメモリカード１１０に鍵生成を指示する（ステップＳ２００）。

【０１６３】メモリカード１１０のコントローラ１４２０は、インタフェース１２０２およびデータバスＢＳ３を介して携帯電話機１００のコントローラ１１０６からの指示を受付け、入力されたデータを鍵生成モジュール１４３２へ送る。そして、鍵生成モジュール１４３２は、入力したデータに基づいて秘密暗号鍵Ｋｉｄと、公開復号鍵ＫＰｉｄとを生成する（ステップＳ２０１）。公開復号鍵ＫＰｉｄは秘密暗号鍵Ｋｉｄと非対称であり、秘密暗号鍵Ｋｉｄで暗号化されたデータを公開復号鍵ＫＰｉｄで復号できることを意味する。

【０１６４】コントローラ１４２０は、生成された秘密暗号鍵Ｋｉｄを鍵生成モジュール１４３２から読出し、Ｋｉｄ保持部１４３３に記録する（ステップＳ２０２）。また、コントローラ１４２０は、生成された公開復号鍵ＫＰｉｄを鍵生成モジュール１４３２から読出し、データバスＢＳ３およびインタフェース１２０２を介してメモリカードインタフェースへ出力する（ステップＳ２０３）。

【０１６５】携帯電話機１００のコントローラ１１０６は、メモリカードインタフェースを介して公開復号鍵ＫＰｉｄを受取り、データバスＢＳ２を介して鍵メモリ１５０８に記録する（ステップＳ２０４）。これで、一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとの生成の動作は終了する。

【０１６６】携帯電話機１００から入力したデータに基づいて、一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとを生成し、秘密暗号鍵Ｋｉｄをメモリカード１１０が保持し、公開復号鍵ＫＰｉｄを携帯電話機１００が保持することにより、メモリカード１１０から携帯電話機１００へ暗号したデータを送付する際に、携帯電話機１００という端末装置固有の情報に基づいて生成された鍵を用いることができ、外部からの進入を防止して暗号化されたデータを十分に保護できる。

【０１６７】図１０のフローチャートでは、携帯電話機１００に入力したデータに基づいて一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとを生成したが、本発明ではこれに限らず、携帯電話機１００のコントローラ１１０６が保持する機器ＩＤまたは電話番号に基づいて一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとを生成しても良い。この場合、ステップＳ２００において、ユーザは操作ボタン部１１０８から鍵生成を指示するための入力を行なう。そうすると、コントローラ１１０６は、その指示を受付け、保持している機器ＩＤまたは電話番号をメモリカードインタフェースを介してメモリカード１１０へ送付する。その後は、図１０に示すフローチャートに従って一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとが生成され、秘密暗号鍵Ｋｉｄがメモリカード１１０のＫｉｄ保持部１４３３で、公開復号鍵ＫＰｉｄが携帯電話機１００の鍵メモリ１５０８で保持される。

【０１６８】また、一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとは、時刻に基づいて生成されても良い。すなわち、ユーザが配信によってメモリカード１１０に記録した暗号化された音楽データを聞きたいと思ったときの時刻に基づいて一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとが生成される。この場合、ステップＳ２００において、ユーザは操作ボタン部１１０８から音楽データの再生指示を入力すると、コントローラ１１０６は、その再生指示を受付けた時刻をタイマー（図示せず）から読取り、メモリカードインタフェースを介してメモリカード１１０へ送付する。その後は、図１０に示すフローチャートに従って一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとが生成され、秘密暗号鍵Ｋｉｄがメモリ１４１５で、公開復号鍵ＫＰｉｄが携帯電話機１００の鍵メモリで保持される。時刻に基づいて一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとが生成されるときは、ユーザが音楽データを聞きたいと思う度ごとに一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとが生成されるため、暗号化されたデータを外部からの進入を防止して十分に保護することができる。

【０１６９】本発明においては、一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとは端末装置（携帯電話機１００）から得られる情報に基づいて生成される。

【０１７０】図１１を参照して、メモリカード１１０に記録された音楽データの再生動作について説明する。再生が開始されると、ユーザは操作ボタン部１１０８から再生指示のための入力を行なう（ステップＳ３００）。携帯電話機１００のコントローラ１１０６は、再生指示を受け取ると。認証データ保持部１５００に保持されている認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａをメモリカード１１０へ入力するように指示する（ステップＳ３０１）。メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを受け取ると、復号処理部１４０８においてＫＰｍａ保持部１４１４に保持された公開認証鍵ＫＰｍａを用いて復号し（ステップＳ３０２）、コントローラ１４２０は、復号処理部１４０８における復号処理結果から、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａが正規の認証データであるか否かを判断する認証処理を行なう。さらに、認証データが正規のデータであった場合、コントローラ１４２０は、クラス証明書Ｃｒｔｆ１がメモリカード１４１５から読出した禁止クラスリストＣＲＬに含まれるか否かを判断する（ステップＳ３０３）。すなわち、認証データが正規の認証データであり、かつ、クラス証明書Ｃｒｔｆ１が禁止クラスリストＣＲＬに含まれない場合、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを承認し、公開暗号鍵ＫＰｐ１とクラス証明書Ｃｒｔｆ１を受理する。

【０１７１】認証データが正規の認証データでない、あ

るいは、認証データが正規の認証データであってもクラス証明書Ｃｒｔｆ１が禁止クラスリストＣＲＬに含まれる場合、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを非承認し、処理を終了する。

【０１７２】公開暗号鍵ＫＰｐ１とクラス証明書Ｃｒｔｆ１を受理すると、コントローラ１４２０は、メモリカードインタフェースを介してメモリカード１１０へ送付する。そうすると、ステップＳ３０４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数に制限がある場合にはアクセス制限情報ＡＣ１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ３０５）。一方、アクセス制限情報ＡＣ１によって再生回数が制限されていない場合においては、ステップＳ３０５はスキップされ、再生制御情報ＡＣ１は更新されることなく処理が次のステップ（ステップＳ３０６）に進行される。

【０１７３】また、ライセンス情報保持部１４４０内にリクエスト曲の当該コンテンツＩＤが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【０１７４】ステップＳ３０４において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリカード１１０のセッションキー発生部１４１８は、セッションキーＫｓ２を発生させる。そして、暗号処理部１４０６は、発生させたセッションキーＫｓ２を、受理した公開暗号鍵ＫＰｐ１を用いて暗号化した｛Ｋｓ２｝Ｋｐ１をデータバスＢＳ３、インタフェース１２０２を介して出力する（ステップＳ３０６）。

【０１７５】携帯電話機１００のコントローラ１１０６の指示に従って、復号処理部１５０１は、Ｋｐ１保持部１５０２に保持された秘密復号鍵Ｋｐ１を用いてメモリカード１１０から得た｛Ｋｓ２｝Ｋｐ１を復号し、得られたセッションキーＫｓ２を受理する（ステップＳ３０７）。そして、携帯電話機１００のセッションキー発生部１５０８は、セッションキーＫｓ３を発生させ、発生させたセッションキーｋｓ３を、受理したセッションキーＫｓ２を用いて暗号化した｛Ｋｓ３｝Ｋｓ２を、メモリカードインタフェースを介してメモリカード１１０に与える（ステップＳ３０８）。

【０１７６】メモリカード１１０のコントローラ１４２０は、インタフェース１２０２に入力された｛Ｋｓ３｝Ｋｓ２を、データバスＢＳ３を介して復号処理部１４１２に与える。復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２を用いて｛Ｋｓ３｝Ｋｓ２を復号し、セッションキーＫｓ３を受理する（ステップＳ３０９）。そしてメモリ１４１５に記録された再生リクエスト曲のライセンスキーＫｃや再生情報の復号処理が実行される。具体的には、コントローラ１４２０の指示に応じて、メモリ１４１５からデータバスＢＳ４に読出された暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１を復号処理部１４２２がメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号し、再生処理に必要なライセンスキーＫｃと再生回路制御情報ＡＣ２がデータバスＢＳ４上に得られる（ステップＳ３１０）。

【０１７７】得られたライセンスキーＫｃと再生回路制御情報ＡＣ２とは、データバスＢＳ３を介して暗号処理部１４３４に送られる。暗号化処理部１４３４は、秘密暗号鍵ＫｉｄによってデータバスＢＳ３から受けたライセンスキーＫｃと再生回路制御情報ＡＣ２を共に暗号化し、｛Ｋｃ／／ＡＣ２｝ＫＰｉｄをデータバスＢＳ４に出力する（ステップＳ３１１）。そして、暗号処理部１４０６は、データバスＢＳ４上の｛Ｋｃ／／ＡＣ２｝ＫＰｉｄを、受理したセッションキーＫｓ３を用いて、さらに暗号化し、暗号化データ｛｛Ｋｃ／／ＡＣ２｝ＫＰｉｄ｝Ｋｓ３をデータバスＢＳ３へ出力する（ステップＳ３１２）。

【０１７８】データバスＢＳ３に出力された暗号化データは、インタフェース１２０２およびメモリカードインタフェースを介して携帯電話機１００に送出される。

【０１７９】携帯電話機１００においては、メモリカードインタフェースを介してデータバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣ２｝ＫＰｉｄを復号処理部１５１０によって復号処理を行ない、暗号化データ｛｛Ｋｃ／／ＡＣ２｝ＫＰｉｄ｝Ｋｓ３を復号処理部１５１４へ出力する（ステップＳ３１３）。復号処理部１５１４は、鍵メモリ１５１２に保持されている公開復号鍵ＫＰｉｄによって復号処理を行ない、ライセンスキーＫｃと再生回路制御情報ＡＣ２とを受理する（ステップＳ３１４）。復号処理部１５１４は、再生回路制御情報ＡＣ２をデータバスＢＳ２に出力する。

【０１８０】コントローラ１１０６は、暗号化データ｛Ｋｃ／／ＡＣ２｝ＫＰｉｄが公開復号鍵ＫＰｉｄを用いて復号されたか否かを判断する（ステップＳ３１５）。この判断は、復号されたデータ列Ｋｃ／／ＡＣ２が最後まで意味のあるデータ列を有するか否かによって行われる。すなわち、暗号化データ｛Ｋｃ／／ＡＣ２｝ＫＰｉｄが鍵メモリ１５１２に保持された公開復号鍵ＫＰｉｄで復号できないときには、復号処理によって発生する余剰データが意味を持たないデータ列になる。したがって、復号の可否を判断することができる。

【０１８１】このとき、暗号化データ｛Ｋｃ／／ＡＣ２｝ＫＰｉｄが復号できないということは、メモリカード１１０内のＫｉｄ保持部１４３３に保持された秘密暗号鍵と携帯電話機１００の鍵メモリ１５１２に保持された公開復号鍵が対応していない、言い換えれば、メモリカード１１０の所有者と携帯電話機１００のユーザとが

異なっていることを意味する。

【０１８２】その後、再生回路制御情報ＡＣ２によって再生の可否が判定される（ステップＳ３１６）。

【０１８３】ステップＳ３１６において、再生回路制御情報ＡＣ２によって再生不可と判断される場合には、再生動作は終了される。

【０１８４】暗号化データ｛Ｋｃ／／ＡＣ２｝ＫＰｉｄが公開復号鍵ＫＰｉｄによって復号でき、かつ、再生回路制御情報によって、携帯電話機１００における再生が許されているとき、携帯電話機１００のコントローラ１１０６は、メモリカードインタフェースを介してメモリカード１１０から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得するための指示を出力する。

【０１８５】そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを読出して（ステップＳ３１７）、データバスＢＳ３およびインタフェース１２０２を介してメモリカードインタフェースへ出力する（ステップＳ３１８）。

【０１８６】携帯電話機１００のコントローラ１１０６は、メモリカードインタフェースを介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、復号処理部１５１６へ入力する。復号処理部１５１６は、入力した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１５１４において復号されたライセンスキーＫｃによって復号し、符号化コンテンツデータＤａｔａを獲得する（ステップＳ３１９）。

【０１８７】復号処理部１５１６は、符号化コンテンツデータＤａｔａを音楽再生部１５１８へ出力し、音楽再生部１５１８は、符号化コンテンツデータＤａｔａを復調して再生する（ステップＳ３２０）。

【０１８８】ＤＡ変換器１５１９は、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換する。そして、再生されたデータは、端子１５２０、スイッチ１５２１を介して増幅器１５２２へ入力され、増幅器１５２２で増幅されて端子１５３０からヘッドホーン１３０等へ出力される。これによって暗号化コンテンツデータの再生動作が終了する。

【０１８９】なお、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの再生は、たとえば、６４ビットづつのブロック単位で行われるため、ステップＳ３１７～Ｓ３２０が、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃが無くなるまで繰返して行われることで音楽が再生される。

【０１９０】上記の説明においては、配信サーバ３０から配信されたライセンスキーＫｃは、メモリカード１１０の鍵生成モジュール１４３２によって生成された秘密暗号鍵Ｋｉｄによって暗号化されずにメモリカード１１０のメモリ１４１５に記録されるが（図９のステップＳ１４４）、再生に必要なライセンスキーＫｃと再生回路制御情報ＡＣ２とを秘密暗号化Ｋｉｄによって暗号化してからメモリ１４１５に記録しても良い。

【０１９１】すなわち、図８および図９に示すフローチャートに従って配信動作が進行し、ステップＳ１４４までの動作が終了すると、図１２に示すように、復号処理部１４２２は、｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１を、秘密復号鍵Ｋｍ１によって復号し、ライセンスキーＫｃ、再生回路制御情報ＡＣ２、ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１のみを受理する（ステップＳ１４６ａ）。

【０１９２】そして、コントローラ１４２０は、受理したライセンスキーＫｃ，再生回路制御情報ＡＣ２と、鍵生成モジュール１４３２からの秘密暗号鍵Ｋｉｄとを暗号処理部１４３４へ入力する。暗号処理部１４３４はライセンスキーＫｃおよび再生回路制御情報ＡＣ２を秘密暗号鍵Ｋｉｄによって暗号化する。コントローラ１４２０は、暗号化データ｛Ｋｃ／／ＡＣ２｝ＫＰｉｄをメモリ１４１５に記録する（ステップＳ１４７）。

【０１９３】その後は、図９のステップＳ１４８以降の動作が実行されて配信動作が終了する。

【０１９４】配信時にコンテンツキーＫｃを秘密暗号鍵Ｋｉｄによって暗号化してメモリ１４１５に記録した場合の暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの再生動作は、図１３に示すように図１１のフローチャートのステップＳ３１１を省略し、ステップＳ３１０をステップ３１０ａに変更したものである。配信時に再生に必要なライセンスキーＫｃと再生回路制御情報ＡＣ２とを秘密暗号鍵Ｋｉｄによって暗号化してメモリ１４１５に記録しておくことにより再生時に復号処理部１４２２と暗号処理部１４３４における処理時間を省略でき、迅速な再生動作が可能である。

【０１９５】メモリカード１１０において生成された秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとはＴＲＭに記録されるため、外部からの進入を排除して一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとを管理できるとともに、一対の秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとを用いて暗号化コンテンツデータを十分に保護しながら再生できる。

【０１９６】上記においては、暗号化コンテンツデータと、暗号化コンテンツデータを復号するライセンスキーとは携帯電話網を用いてメモリカード１１０に配信されると説明したが、それ以外の方法によって配信されても良い。

【０１９７】図１４を参照して、コンピュータ１４０を用いた暗号化コンテンツデータの配信について説明する。携帯電話機１００にはメモリカード１１０が着脱可能であり、音楽を再生するためのヘッドホーン１３０が接続されている。そして、携帯電話機１００は、通信ケーブル１４５を介してコンピュータ１４０と接続されている。

【０１９８】コンピュータ１４０は、ハードディスク１４１と、コントローラ１４２と、外部インタフェース１４３とを備える。そして、ハードディスク１４１はデータバスＢＳ５を介してコントローラ１４２と接続され、コントローラ１４２はライセンス保護モジュール１４３を含む。

【０１９９】ハードディスク１４１は、インターネット配信によってコンピュータ１４０に配信された暗号化コンテンツデータをデータバスＢＳ５を介して記憶する。コントローラ１４２は、携帯電話機１００のユーザから通信ケーブル１４５および外部インタフェース１４３を介して暗号化コンテンツデータの送信要求があると、ハードディスク１４１から暗号化コンテンツデータを読出し、外部インタフェース１４３を介して外部へ出力する。

【０２００】外部インタフェース１４３は、携帯電話機１００から通信ケーブル１４５を介してコンピュータ１４０に入力された信号をコントローラ１４２に入力するとともに、コントローラ１４２からの信号を外部へ出力する。

【０２０１】ライセンス保護モジュール１４４は、図５に示すデータ処理部３１０と同じ構成を有し、携帯電話機１００に装着されたメモリカード１１０に暗号化コンテンツデータを送信するために、上述したように携帯電話機１００およびメモリカード１１０と公開暗号鍵、セッションキー等のやり取りを行ないながら、暗号化コンテンツデータを保護してメモリカード１１０へ送信するものである。

【０２０２】インターネット配信によって配信サーバからコンピュータ１４０に暗号化コンテンツデータが配信され、コンピュータ１４０のハードディスク１４１にデータバスＢＳ５を介して暗号化コンテンツデータが記憶されている。

【０２０３】携帯電話機１００のユーザが操作ボタン部１１０８から送信要求を入力すると、通信ケーブル１４５および外部インタフェース１４３を介して送信要求がコントローラ１４２に入力される。コントローラ１４２は、送信要求を受付けると、要求された暗号化コンテンツデータをデータバスＢＳ５を介してハードディスク１４１から読出し、ライセンス保護モジュール１４４に入力する。

【０２０４】ライセンス保護モジュール１４４は、上述したようにメモリカード１１０と通信ケーブル１４５を介して公開暗号鍵、セッションキー等のやり取りを行ない、暗号化コンテンツデータをメモリカード１１０へ送信する。

【０２０５】送信後、携帯電話機１００のユーザは、上述したのと同じ方法によって暗号化コンテンツデータを再生する。

【０２０６】また、コンピュータ１４０は、インターネット配信によって暗号化コンテンツデータを受信しなくても良く、暗号化コンテンツデータが記録されたＣＤ－ＲＯＭをコンピュータ１４０に接続されたＣＤ－ＲＯＭドライブ（図示せず）に装着し、そのＣＤ－ＲＯＭから暗号化コンテンツデータを読出してメモリカード１１０へ送信しても良い。また、ＣＤ－ＲＯＭに記録された暗号化コンテンツデータを、一旦、ハードディスク１４１に記憶しておいても良い。

【０２０７】なお、図１４において、コンピュータ１４０は暗号化コンテンツデータを復号するためのコンテンツキーを携帯電話機１００へ送信しない。コンテンツキーは、別途、携帯電話網等を介して携帯電話機１００へ配信され、その時、著作権料が課金される。

【０２０８】さらに、コンピュータ１４０は、ＣＤリッピングによって暗号化コンテンツデータとライセンスを生成しても良い。リッピングとは、音楽ＣＤから取得した音楽データを、音楽再生モジュールで再生できるように変換することを言う。まず、取得した音楽データに対してライセンスを生成する。次いで、取得した音楽データを音楽再生部１５１８にて再生可能なコンテンツデータに変換した後、生成したライセンスに含まれるコンテンツキーにて復号可能な暗号化を行なうもので、リッピングによって得られた暗号化コンテンツデータの生成されたライセンスには、複製ができないように管理される。したがって、音楽ＣＤからの１次複製であるＣＤリッピングは、コンテンツの暗号化と、その復号鍵であるコンテンツキーを含むライセンスが複製できない構成を取ることで著作権を保護した適法な行為である。

【０２０９】ＣＤを用いた場合、音楽ＣＤから取得して生成した暗号化コンテンツデータとライセンスは、一旦、ハードディスク１４１に記録してからメモリカード１１０へ送信しても良いし、ハードディスク１４１に送信せずに、直接、メモリカード１１０へ送信しても良い。

【０２１０】暗号化コンテンツデータは、図１５に示すようにメモリカード１１０を、直接、コンピュータ１４０に装着してメモリカード１１０に暗号化コンテンツデータを記録しても良い。この場合、コンピュータ１４０のコントローラ１４２は、ライセンス保護モジュール１４４によって、直接、メモリカード１１０に暗号化コンテンツデータを記録する。

【０２１１】図１５においても、コンピュータ１４０は、図１４に示す場合と同じ方法により暗号化コンテンツデータを取得する。

【０２１２】なお、上記説明においては、秘密暗号鍵Ｋｉｄと公開復号鍵ＫＰｉｄとは、携帯電話機１００のＩＤ、および携帯電話機１００の電話番号等の携帯電話機１００から入力された情報に基づいて非対称に生成されると説明したが、本発明においては、これに限らず、共通鍵方式のように、携帯電話機１００のＩＤ、および携

帯電話機１００の電話番号等の携帯電話機１００から入力された情報に基づいて対称に生成されてもよい。

【０２１３】実施の形態として暗号化されたコンテンツデータと、その復号鍵であるライセンスキーを含むライセンスを記録するメモリカードにおけるライセンスの記録あるいは出力における暗号を用いたライセンスの受け渡しによるコンテンツ保護について説明したが、ライセンスを用いないでコンテンツデータの記録あるいは出力において暗号を用いて保護するようにしても同様の効果が得られる。

【０２１４】さらに、音楽データや画像データなどのコンテンツデータのみでなくデータ全般に対しても適用することが可能である。

【０２１５】また、コントローラを備えたメモリカードに限らず、コントローラを備えたハードディスク等の他の記録媒体であっても適用可能である。

【０２１６】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

【図５】　ライセンスサーバの構成を示す概略ブロック図である。

【図６】　実施の形態による携帯電話機の構成を示すブロック図である。

【図７】　実施の形態によるメモリカードの構成を示すブロック図である。

【図８】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図９】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１０】　携帯電話機から入力した情報に基づく一対の秘密暗号鍵と公開復号鍵との生成を説明するためのフローチャートである。

【図１１】　実施の形態における携帯電話機における再生動作を説明するためのフローチャートである。

【図１２】　図１に示すデータ配信システムにおける配信動作を説明するための他の第２のフローチャートである。

【図１３】　実施の形態における携帯電話機における再生動作を説明するための他のフローチャートである。

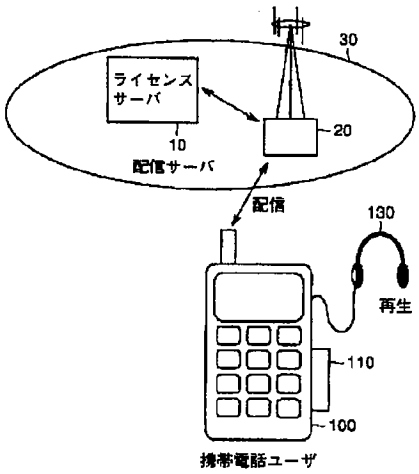
【図１４】　他のデータ配信システムを概念的に説明する概略図である。

【図１５】　さらに他のデータ配信システムを概念的に説明する概略図である。

【符号の説明】

１０　ライセンスサーバ、２０　配信キャリア、３０　配信サーバ、１００携帯電話機、１１０　メモリカード、１３０　ヘッドホーン、１４０　コンピュータ、１４１　ハードディスク、１４２，１１０６，１４２０　コントローラ、１４３，１１０７　外部インタフェース、１４４，１４５０　ライセンス保護モジュール、１４５　通信ケーブル、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１４，１５１６　復号処理部、３１５　配信制御部、３１６，１４１８，１５０８セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４３４，１５０６　暗号処理部、３５０　通信装置、１１０２　アンテナ、１１０４　送受信部、１１０８　操作ボタン部、１１１０　ディスプレイ、１１１２音声再生部、１１１３，１５１９　ＤＡ変換器、１１１４，１５２０，１５３０端子、１２００　メモリカードインタフェース、１２０２　インタフェース、１４０２　Ｋｍｃ１保持部、１４１４　ＫＰｍａ保持部、１４１５　メモリ、１４１６　ＫＰｍ１保持部、１４２１　Ｋｍ１保持部、１４４０　ライセンス情報保持部、１４４２，１４４４，１４４６　切換スイッチ、１４００，１５００認証データ保持部、１４３２　鍵生成モジュール、１４３３　Ｋｉｄ保持部、１５０２　Ｋｐ１保持部、１５１２　鍵メモリ、１５１８　音楽再生部、１５２１スイッチ、１５２２　増幅器、１５５０　音楽再生モジュール。

【図１】



【図２】

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツ データ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化 コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいは サーバアクセス関連等の平文情報
コンテンツ ID	コンテンツに関する 情報		コンテンツデータDataを識別するコード
ライセンス ID	ライセンスに関する 情報		ライセンスの発行を特定できる管理コード （コンテンツIDを含めて識別することも可）
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報 （例：再生可否）

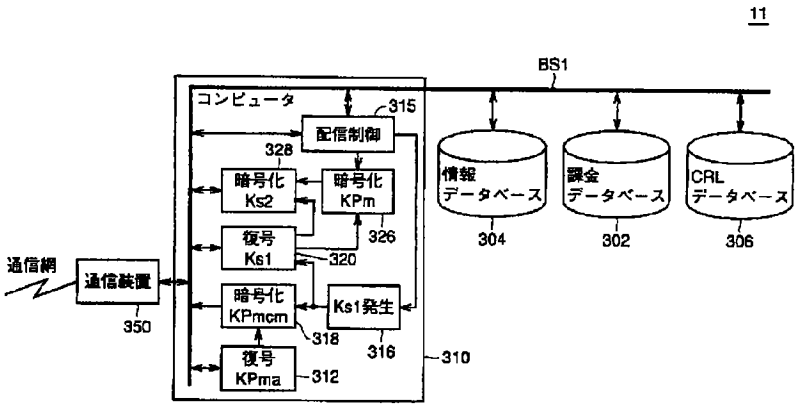
【図３】

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト 関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 （差分データ形式）
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 （非対称鍵）	携帯電話機	Kpnにて復号可能。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機の種類nごとに異なる。
KPmcm	公開暗号鍵 （非対称鍵）	メモリカード	Kmcmにて復号可能。 {KPmcm//Cmcm}KPmaの形式で出荷時に記録 ＊メモリカードの種類mごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 ＊携帯電話機の種類nごとに異なる。
Kmcm	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ＊メモリカードの種類mごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 認証データ{KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機のクラスnごとに異なる。
Cmcm		メモリカード	メモリカードのクラス証明書。認証機能を有する。 認証データ{KPmcm//Cmcm}KPmaの形式で出荷時に記録 ＊メモリカードのクラスmごとに異なる。

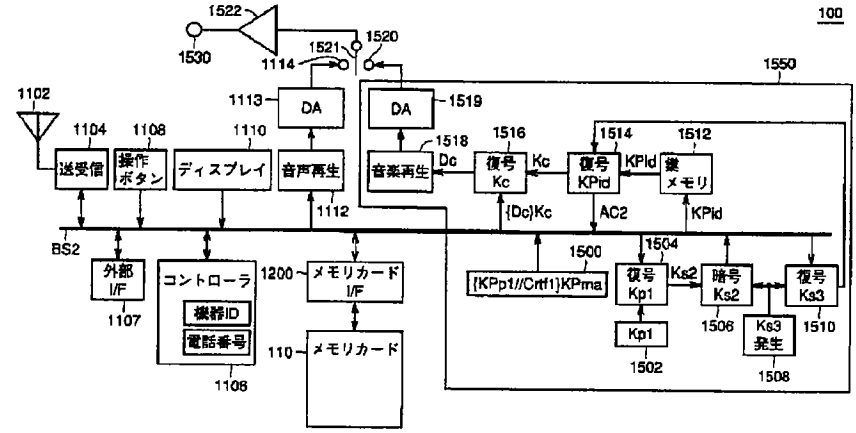
【図４】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 （非対称鍵）	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。
KPid	公開復号鍵	携帯電話機 メモリカード	携帯電話機から得られる情報に基づいて 生成され、再生セッションに用いられる。
Kid	秘密暗号鍵	メモリカード	携帯電話機から得られる情報に基づいて 生成され、再生セッションに用いられる。

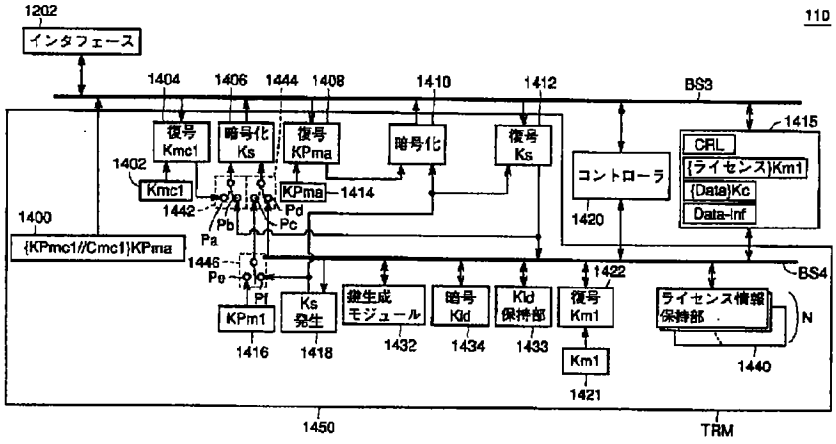
【図５】



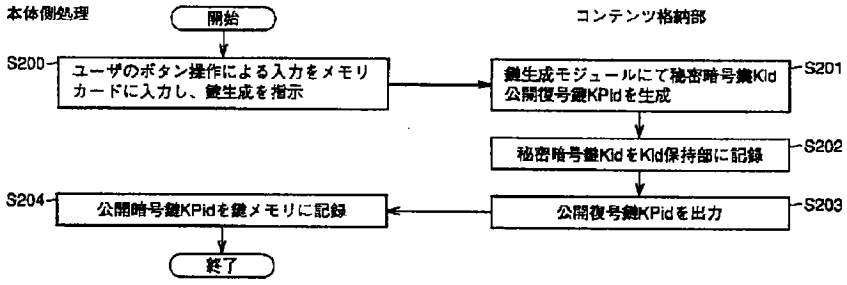
【図６】



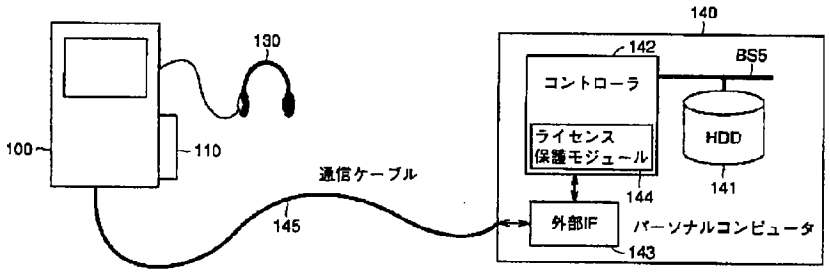
【図７】


1202
インタフェース
110
1404
1406
1444
1408
1410
1412
BS3
1415
CRL
{ライセンス}Km1
{Data}Kc
Data-Inf
復号 Kmc1
暗号化 Ks
復号 KPma
暗号化
復号 Ks
コントローラ
1420
1402
Kmc1
KPma
1414
1442
Pd
Pb
Pc
Pa
1400
{KPmc1//Cmc1}KPma
1446
Pe
Pf
BS4
1422
KPm1
Ks 発生
鍵生成 モジュール
暗号 Kld
Kld 保持部
復号 Km1
ライセンス情報 保持部
N
1416
1418
1432
1434
1433
Km1
1421
1440
1450
TRM

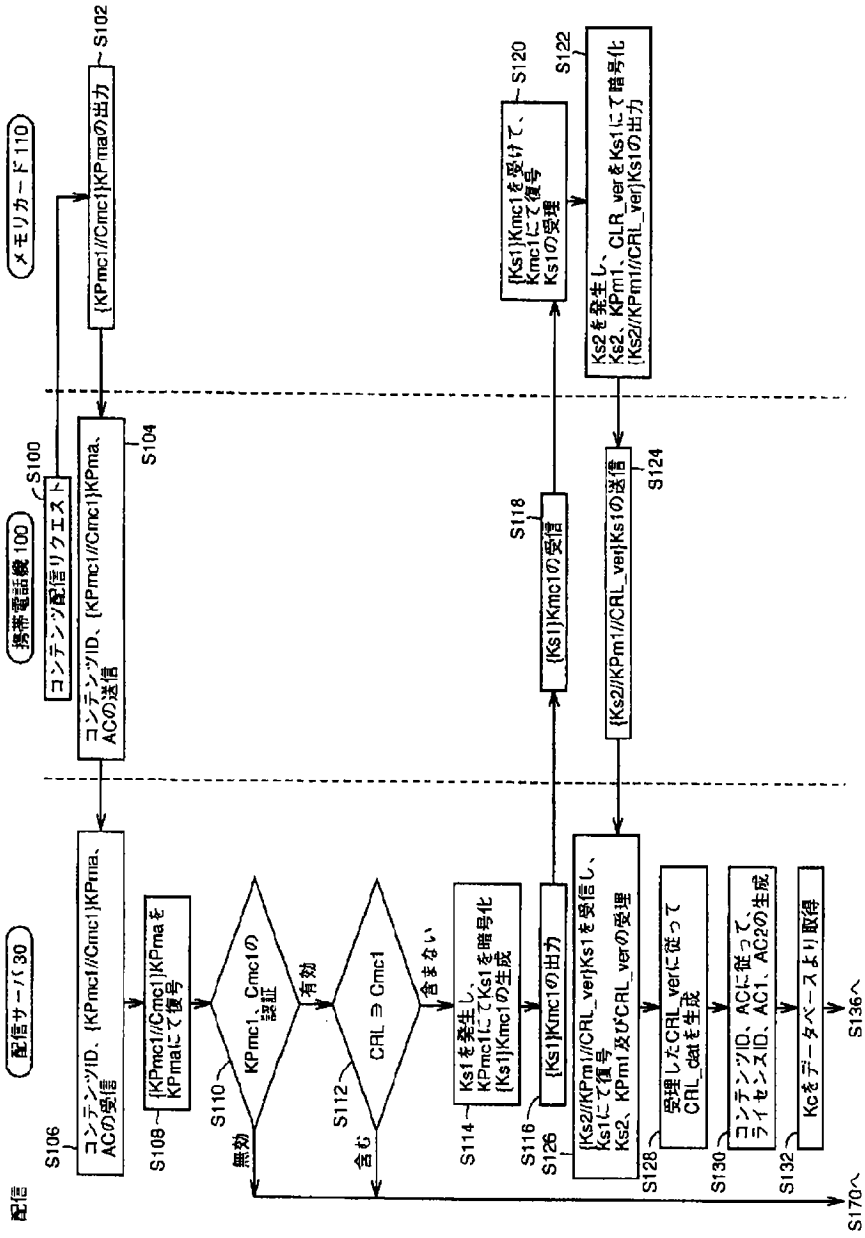
【図１０】


本体側処理
開始
コンテンツ格納部
S200
ユーザのボタン操作による入力をメモリカードに入力し、鍵生成を指示
鍵生成モジュールにて秘密暗号鍵Kld 公開復号鍵KPidを生成
S201
秘密暗号鍵KldをKld保持部に記録
S202
S204
公開暗号鍵KPidを鍵メモリに記録
公開復号鍵KPidを出力
S203
終了

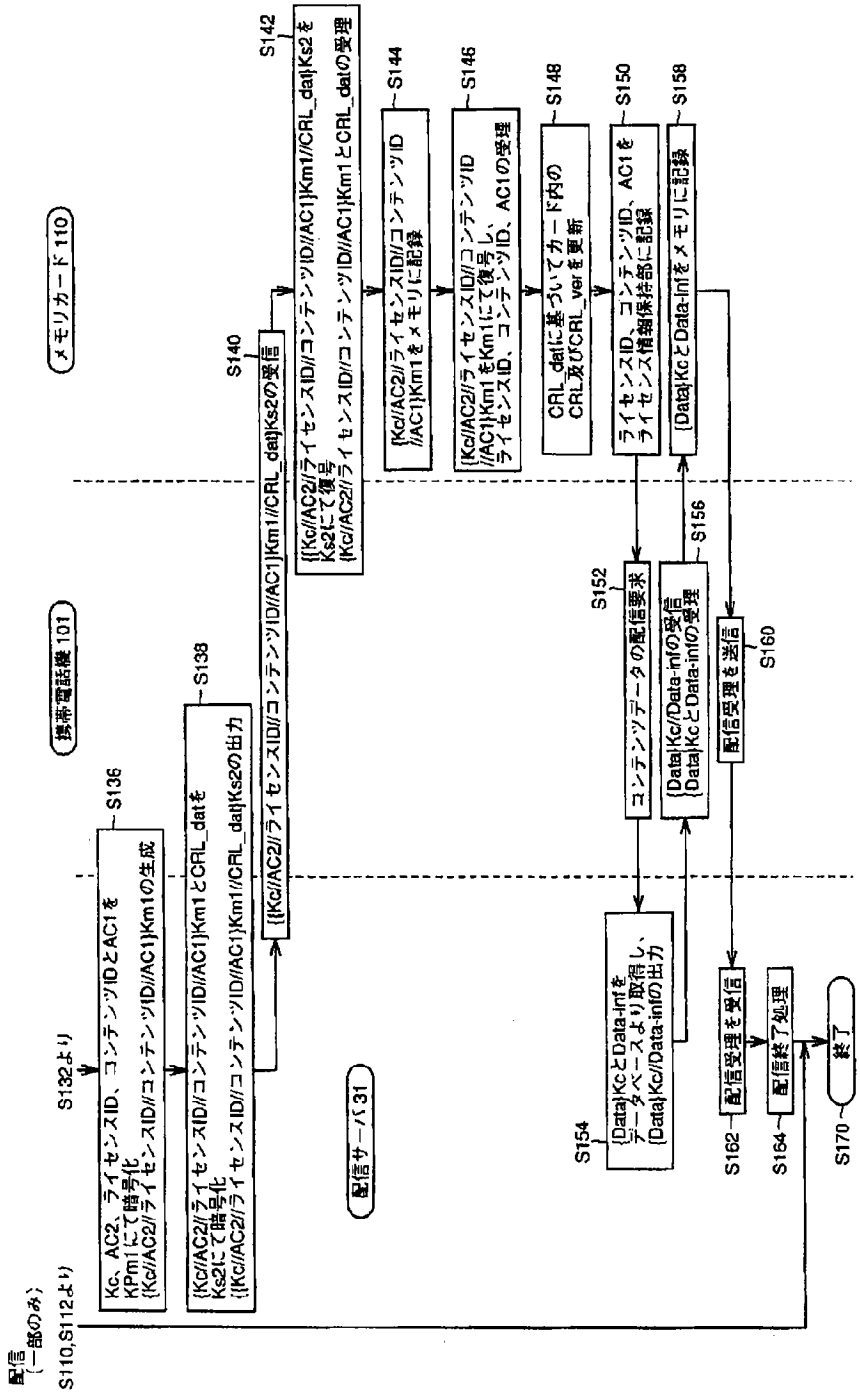
【図１４】


140
130
142
BS5
コントローラ
HDD
100
110
ライセンス 保護モジュール
通信ケーブル
144
141
145
外部IF
パーソナルコンピュータ
143

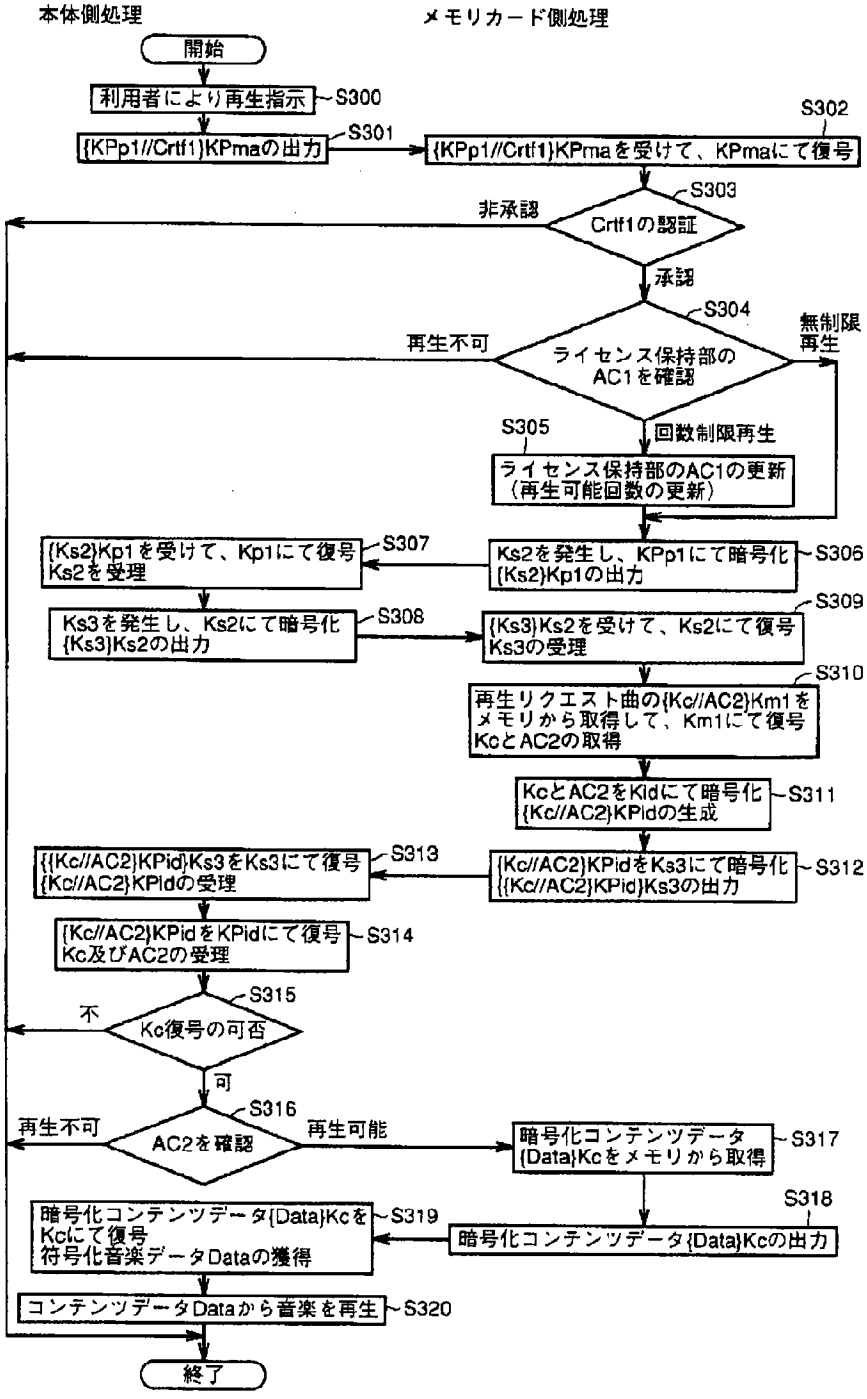
【図８】


配信
配信サーバ30
携帯電話機100
メモリカード110
S100
コンテンツ配信リクエスト
S102
{KPmc1//Cmc1}KPmaの出力
S104
コンテンツID、{KPmc1//Cmc1}KPma、ACの送信
S106
コンテンツID、{KPmc1//Cmc1}KPma、ACの受信
S108
{KPmc1//Cmc1}KPmaをKPmaにて復号
S110
KPmc1、Cmc1の認証
無効
有効
S112
CRL ∋ Cmc1
含む
含まない
S114
Ks1を発生し、KPmc1にてKs1を暗号化{Ks1}Kmc1の生成
S116
{Ks1}Kmc1の出力
S118
{Ks1}Kmc1の受信
S120
{Ks1}Kmc1を受けて、Kmc1にて復号Ks1の受理
S122
Ks2を発生し、Ks2、KPm1、CLR_verをKs1にて暗号化{Ks2//KPm1//CRL_ver}Ks1の出力
S124
{Ks2//KPm1//CRL_ver}Ks1の送信
S126
{Ks2//KPm1//CRL_ver}Ks1を受信し、Ks1にて復号Ks2、KPm1及びCRL_verの受理
S128
受理したCRL_verに従ってCRL_datを生成
S130
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S132
Kcをデータベースより取得
S136へ
S170へ

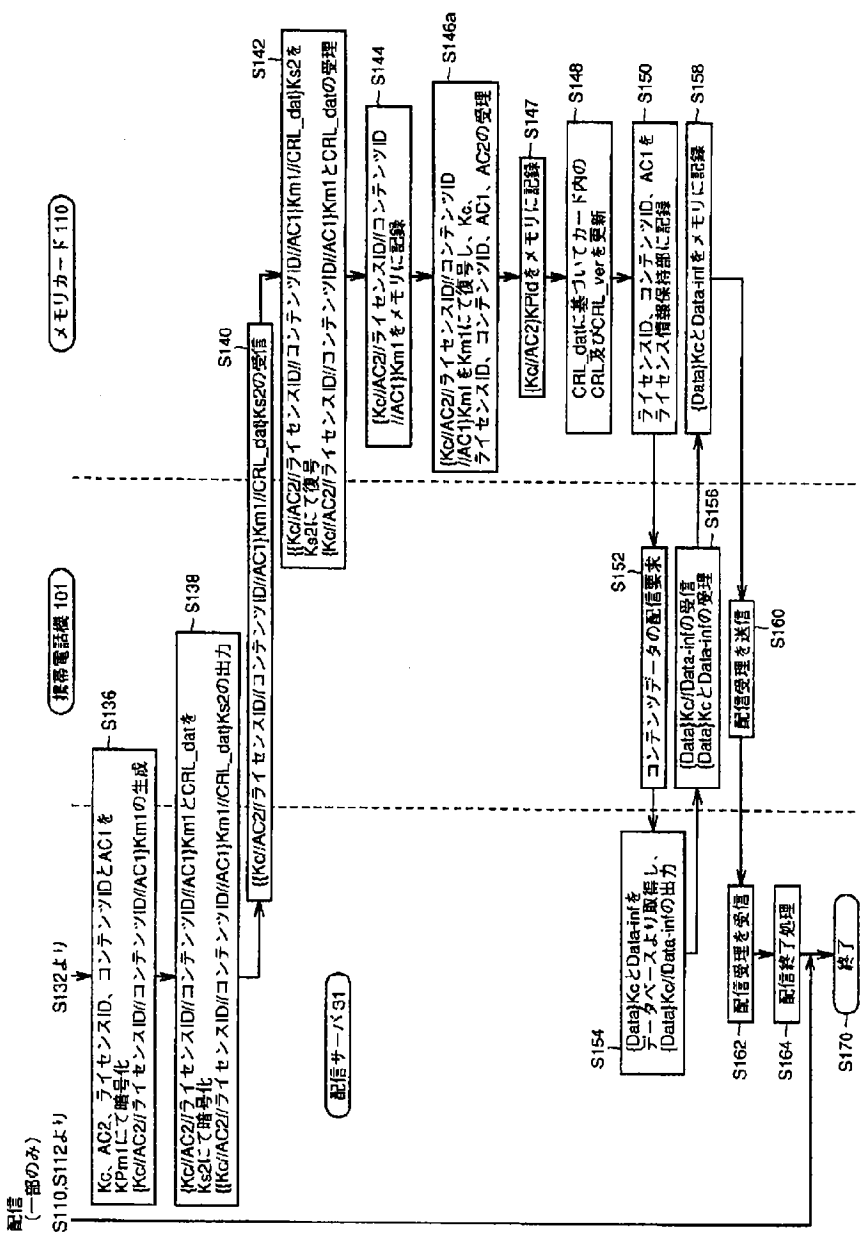
【図９】


配信
(一部のみ)
S110,S112より
携帯電話機101
メモリカード110
配信サーバ31
S132より
S136
Kc、AC2、ライセンスID、コンテンツIDとAC1を
KPm1にて暗号化
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1の生成
S138
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datを
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の出力
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受信
S140
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datの受理
S142
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をメモリに記録
S144
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をKm1にて復号し、
ライセンスID、コンテンツID、AC1の受理
S146
CRL_datに基づいてカード内の
CRL及びCRL_verを更新
S148
ライセンスID、コンテンツID、AC1を
ライセンス情報保持部に記録
S150
{Data}KcとData-infをメモリに記録
S158
S152
コンテンツデータの配信要求
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S156
配信受理を送信
S160
S154
{Data}KcとData-infを
データベースより取得し、
{Data}Kc//Data-infの出力
S162
配信受理を受信
S164
配信終了処理
S170
終了

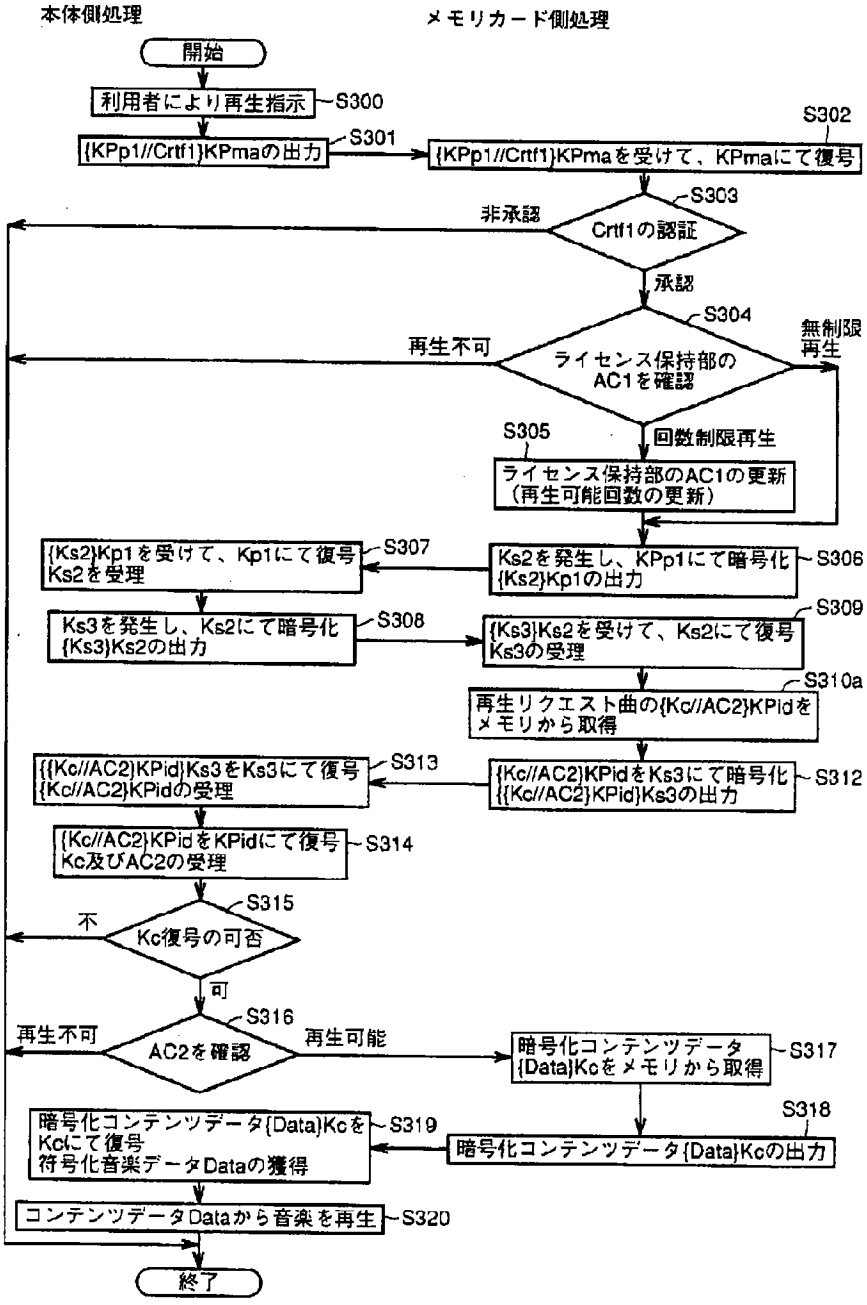
【図１１】


本体側処理
メモリカード側処理
開始
利用者により再生指示
S300
{KPp1//Crtf1}KPmaの出力
S301
{KPp1//Crtf1}KPmaを受けて、KPmaにて復号
S302
Crtf1の認証
S303
非承認
承認
ライセンス保持部のAC1を確認
S304
再生不可
無制限再生
回数制限再生
S305
ライセンス保持部のAC1の更新（再生可能回数の更新）
Ks2を発生し、KPp1にて暗号化{Ks2}Kp1の出力
S306
{Ks2}Kp1を受けて、Kp1にて復号Ks2を受理
S307
Ks3を発生し、Ks2にて暗号化{Ks3}Ks2の出力
S308
{Ks3}Ks2を受けて、Ks2にて復号Ks3の受理
S309
再生リクエスト曲の{Kc//AC2}Km1をメモリから取得して、Km1にて復号KcとAC2の取得
S310
KcとAC2をKidにて暗号化{Kc//AC2}KPidの生成
S311
{Kc//AC2}KPidをKs3にて暗号化{{Kc//AC2}KPid}Ks3の出力
S312
{{Kc//AC2}KPid}Ks3をKs3にて復号{Kc//AC2}KPidの受理
S313
{Kc//AC2}KPidをKPidにて復号Kc及びAC2の受理
S314
Kc復号の可否
S315
不
可
AC2を確認
S316
再生不可
再生可能
暗号化コンテンツデータ{Data}Kcをメモリから取得
S317
暗号化コンテンツデータ{Data}Kcの出力
S318
暗号化コンテンツデータ{Data}Kcを Kcにて復号 符号化音楽データDataの獲得
S319
コンテンツデータDataから音楽を再生
S320
終了

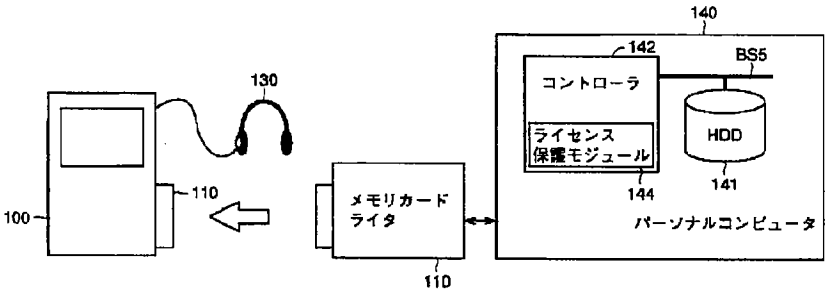
【図１２】


配信
(一部のみ)
S110,S112より
S132より
携帯電話機 101
メモリカード 110
配信サーバ 31
S136
Kc、AC2、ライセンスIDとAC1を
KPmに暗号化
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1の生成
S138
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datを
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の出力
S140
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受信
S142
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datの受理
S144
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をメモリに記録
S146a
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をKm1にて復号し、Kc、
ライセンスID、コンテンツID、AC1、AC2の受理
S147
{Kc//AC2}KPidをメモリに記録
S148
CRL_datに基づいてカード内の
CRL及びCRL_verを更新
S150
ライセンスID、コンテンツID、AC1を
ライセンス情報保持部に記録
S158
{Data}KcとData-infをメモリに記録
S152
コンテンツデータの配信要求
S154
{Data}KcとData-infを
データベースより取得し、
{Data}Kc//Data-infの出力
S156
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S160
配信受理を送信
S162
配信受理を受信
S164
配信終了処理
S170
終了

【図１３】


本体側処理
メモリカード側処理
開始
利用者により再生指示
S300
{KPp1//Crtf1}KPmaの出力
S301
{KPp1//Crtf1}KPmaを受けて、KPmaにて復号
S302
Crtf1の認証
S303
非承認
承認
ライセンス保持部のAC1を確認
S304
再生不可
無制限再生
回数制限再生
S305
ライセンス保持部のAC1の更新（再生可能回数の更新）
Ks2を発生し、KPp1にて暗号化{Ks2}Kp1の出力
S306
{Ks2}Kp1を受けて、Kp1にて復号Ks2を受理
S307
Ks3を発生し、Ks2にて暗号化{Ks3}Ks2の出力
S308
{Ks3}Ks2を受けて、Ks2にて復号Ks3の受理
S309
再生リクエスト曲の{Kc//AC2}KPidをメモリから取得
S310a
{Kc//AC2}KPidをKs3にて暗号化{{Kc//AC2}KPid}Ks3の出力
S312
{{Kc//AC2}KPid}Ks3をKs3にて復号{Kc//AC2}KPidの受理
S313
{Kc//AC2}KPidをKPidにて復号Kc及びAC2の受理
S314
Kc復号の可否
S315
不
可
AC2を確認
S316
再生不可
再生可能
暗号化コンテンツデータ{Data}Kcをメモリから取得
S317
暗号化コンテンツデータ{Data}Kcの出力
S318
暗号化コンテンツデータ{Data}Kcを Kcにて復号 符号化音楽データDataの獲得
S319
コンテンツデータDataから音楽を再生
S320
終了

【図１５】



フロントページの続き

(51) Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
		Ｈ０４Ｎ　7/167	Ｚ

(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

Ｆターム(参考)　5B085 AE02 AE12 AE13 AE23 AE29
5C064 CB08
5J104 AA01 AA07 AA16 EA04 KA05
KA10 MA02 NA02 PA02 PA07
PA14
5K067 AA30 BB04 DD17 DD52 DD54
FF04 FF07 FF40 HH23 HH24
HH36 KK15